NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 8715.3C
Effective Date: March 12, 2008
Expiration Date: March 12, 2013

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA General Safety Program Requirements (w/Change 7 dated 2/25/11)

Responsible Office: Office of Safety and Mission Assurance

| TOC | ChangeLog | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | ALL |

Appendix F. Sample System Safety Technical Plan for Systems Acquisition, Research, and Development Programs

The NASA program manager (or designee) will publish and maintain an approved System Safety Technical Plan (SSTP) that includes a risk management plan, appropriate to and for the life of the program. This plan may be incorporated in the more comprehensive safety and mission assurance plan, mission assurance plan, or other plan, provided that the required data are identifiable and complete.

1. The SSTP defines the objectives, responsibilities, and methods to be used for overall safety program conduct and risk management control. Integration of system/facility safety provisions into the SSTP is vital to the early implementation and ultimate success of the safety effort. Inclusion of these provisions in the plan will send an unmistakable message to all program participants that safety and risk management are an integral part of the management process and all tasks. The authority to conduct the safety program must originate in the respective SSTP governing each NASA program.

2. The program SSTP will be the vehicle for safety and risk management task planning. The plan should include detailed task requirements for each system safety task, as appropriate for the program. The NASA program organization and system safety relationships and responsibilities will be described along with reporting channels for this task. In particular, the plan will show how NASA will manage its independent safety

oversight role. The plan will stipulate the specifics of the system safety modeling activities and describe what and how safety adverse consequences will be modeled, how system safety models (qualitative and probabilistic risk assessments) will be integrated and applied for risk-informed decision making and safety monitoring, how the technical team(s) responsible for generating and maintaining system safety models will interact with the system engineering organizations, the reporting and approval protocol, and the cost and schedule associated with accomplishing system safety modeling activities in relation to the critical or key events during all phases of the life cycle. It will also address requirements for NASA and contractor participation in design, safety, and readiness reviews. The program SSTP should be a compliance document in the request for proposal. Data requirements for the program SSTP are in the data requirements document. For a multi-Field Installation program, each Center should provide a supplement to the plan to ensure compatibility among Field Installation organizations and the ability to comply with task requirements.

3. The level of safety directly correlates with management's emphasis on the safety of the system/facility being developed. Proper identification of the system/facility safety program elements is the first step towards developing a successful program. Each functional safety program will have the following basic elements:

a. Requirement management.

b. System safety modeling activities (system safety, risk assessment, uncertainty assessment)

c. Data collection and analysis activities.

d. Decision-making process to manage and monitor risk.

e. Implementation (planning, organization, interface/coordination, and reporting).

4. Each of these elements is aligned with an overall approach to risk evaluation by:

a. Identifying system/facility safety hazards.

b. Determining the risk scenarios associated with the hazard.

c. Assessing the probabilities and consequences associated with the risk scenarios.

d. Assessing the uncertainties associated with the probabilities and consequences.

e. Determining risk control strategies to either eliminate or control the safety hazard.

f. Recommending corrective action or alternatives to the appropriate management level for a decision to either eliminate the hazard or accept the risk. Risks acceptance is the responsibility of the program manager. In all cases, notification of risk acceptance will be communicated to the next higher authority (see Chapter 2).

g. Documenting those areas in which a decision has been made to accept the risk, including the rationale for the risk acceptance.

5. During the concept development phase, appropriate safety tasks should be planned that will become the foundation for safety efforts and risk management efforts during system definition, design, manufacture, test, and operations.

a. Identify special safety studies and risk assessments that may be required during system definition or design.

b. Estimate gross personnel requirements for the safety program for the complete system life cycle.

c. Perform trade studies by using the results of hazard analyses and risk assessments that identify high hazardous areas or identify high risk sensitivities, with recommended alternatives.

d. Establish safety and risk goals and objectives that will be used to determine the type of safety and risk inputs for the overall program.

(1) The goals should be measurable and state what would be accomplished by performing the various safety tasks and risk management tasks.

(2) The goals should be structured so that safety tasks and risk management tasks can be selected to accomplish them.

(3) Task results should clearly demonstrate that the goals have been met.

e. Complete hazard analyses and risk assessments to identify potentially hazardous systems and to develop initial safety requirements and risk management criteria. f. Continuously review hardware procedural requirements and concepts to maintain an understanding of the evolving system.

g. Use pertinent historical data from similar systems as input to the risk assessment and to refine initial evaluations.

| TOC | ChangeLog | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS